Unextendible Mutually Unbiased Bases from Pauli Classes

Prabha Mandayam
The Institute of Mathematical Sciences, Taramani, Chennai - 600113, India.

Somshubhro Bandyopadhyay
Department of Physics and Center for Astroparticle Physics and Space Science, Bose Institute, Bidhan Nagar, Kolkata - 700091, India.

Markus Grassl
Centre for Quantum Technologies, National University of Singapore, Singapore 117543, Singapore.

William K. Wootters
Department of Physics, Williams College, Williamstown, MA - 01267, USA.
(Dated: February 18, 2013)

We provide a construction of sets of $d/2+1$ mutually unbiased bases (MUBs) in dimensions $d = 4, 8$ using maximal commuting classes of Pauli operators. We show that these incomplete sets cannot be extended further using the operators of the Pauli group. However, specific examples of sets of MUBs obtained using our construction are shown to be *strongly unextendible*; that is, there does not exist another vector that is unbiased with respect to the elements in the set. We conjecture the existence of such unextendible sets in higher dimensions $d = 2^n (n > 3)$ as well.

Furthermore, we note an interesting connection between these unextendible sets and state-independent proofs of the Kochen-Specker Theorem for two-qubit systems. Our construction also leads to a proof of the tightness of a H_2 entropic uncertainty relation for any set of three MUBs constructed from Pauli classes in $d = 4$.

I. INTRODUCTION

Two orthonormal bases $\mathcal{A} = \{|a_i\rangle, i = 1, \ldots, d\}$ and $\mathcal{B} = \{|b_j\rangle, j = 1, \ldots, d\}$ of the d-dimensional Hilbert space $\mathbb{C}^d$ are said to be *mutually unbiased* if for every pair of basis vectors $|a_i\rangle \in \mathcal{A}$ and $|b_j\rangle \in \mathcal{B}$,

$$|\langle a_i|b_j\rangle| = \frac{1}{\sqrt{d}}, \forall i, j = 1, \ldots, d. \tag{1}$$

Two bases $\mathcal{A}$ and $\mathcal{B}$ that are mutually unbiased have the property that if a physical system is prepared in an eigenstate of basis $\mathcal{A}$ and measured in basis $\mathcal{B}$, all outcomes are equally probable. A set of orthonormal bases $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m\}$ in $\mathbb{C}^d$ is called a set of mutually unbiased bases (MUBs) if every pair of bases in the set is mutually unbiased. MUBs play an important role in our understanding of complementarity in quantum mechanics and are central to several key quantum information processing tasks including quantum cryptography and state tomography.

MUBs form a minimal and optimal set of orthogonal measurements for quantum state tomography [1, 2]. To specify a general density matrix $\rho \in \mathbb{C}^d$, which is Hermitian and has $\mathrm{Tr}(\rho) = 1$, one needs $d^2 - 1$ real parameters. Since measurements within a particular basis set can yield only $d - 1$ independent probabilities, one needs $d + 1$ distinct basis sets to provide the required total number of $d^2 - 1$ independent probabilities. Correspondingly, the maximal number of MUBs that can exist in d-dimensional Hilbert space is $d + 1$ and explicit constructions of such maximal sets are known when d is a prime power [2–4]. However, in composite dimensions while smaller sets of MUBs have been constructed [5, 6], the question as to whether a complete set of MUBs exists in non-prime-power dimensions still remains unresolved.

MUBs also play an important role in quantum cryptographic protocols, since they correspond to measurement bases that are most 'incompatible', as quantified by uncertainty relations. A set of measurement bases is said to be *maximally incompatible* if they satisfy a maximally strong uncertainty relation. Being mutually unbiased is a necessary condition for a set of measurement bases to be maximally incompatible [7]. The security of cryptographic tasks such as quantum key distribution [8] and two-party protocols using the noisy-storage model [9] relies on this property of MUBs. In particular, protocols based on higher-dimensional quantum systems with larger numbers of unbiased basis sets can have certain advantages over those based on qubits [10, 11]. It is therefore important for cryptographic applications to find sets of MUBs that satisfy strong uncertainty relations.

Related to the question of finding complete sets of MUBs is the important concept of *unextendible* MUBs. A set of MUBs $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m\}$ in $\mathbb{C}^d$ is said to be *unextendible* if there does not exist another basis in $\mathbb{C}^d$ that is unbiased with respect to all the bases $\mathcal{B}_j, j = 1, \ldots, m$. In this paper we show the existence of unextendible sets of MUBs even in systems for which a complete set of MUBs is known to exist.

We follow a standard construction of MUBs based on finding mutually disjoint, maximal commuting classes of tensor products of Pauli operators [3, 4]. It is always possible to find a partitioning of the n-qubit Pauli operators in $d = 2^n$ into $d+1$ disjoint maximal commuting classes,

the common eigenbases of which form a complete set of $d+1$ MUBs [3, 4]. Here, we show that there exist smaller sets of $k < d+1$ commuting classes $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_k\}$ in $d = 4, 8$ that are *unextendible* in the following sense—no more maximal commuting classes can be formed out of the remaining n-qubit Pauli operators that are not contained in $\mathcal{C}_1 \cup \mathcal{C}_2 \ldots \cup \mathcal{C}_k$. The eigenbases of $\{\mathcal{C}_1, \ldots, \mathcal{C}_k\}$ thus give rise to a set of k MUBs which cannot be extended using joint eigenvectors of maximal sets of commuting Paulis. We call such sets *weakly unextendible*.

We also obtain examples of *strongly unextendible* sets of MUBs using our construction of unextendible classes in $d = 4, 8$, that is, there does not exist even a single vector unbiased with respect to the bases in these sets. For two-qubit systems, our construction of unextendible sets of maximal commuting Pauli classes enables us to prove the tightness of an entropic uncertainty relation. Furthermore, we also demonstrate an interesting connection between unextendible sets of classes and state-independent proofs of the Kochen-Specker Theorem [12, 13].

The rest of the paper is organized as follows. We formally define weak and strong unextendibility in Section II and review the standard construction of MUBs from maximal Pauli classes. In Section III we state our main results on constructing unextendible Pauli classes in $d = 4, 8$, detailed proofs of which are given in the Appendix (Sections A, B). In Section IV we present examples of sets of MUBs obtained using our construction that are in fact strongly unextendible. Finally, we discuss properties and potential applications of such unextendible sets in Section V.

II. PRELIMINARIES

A. Construction of MUBs from Maximal Commuting Operator Classes

Let $\mathcal{S}$ be a set of d^2 mutually orthogonal [19] unitary operators in $\mathbb{C}^d$. This set of d^2 operators (including the identity operator $\mathbb{I}$) constitutes a basis for the space of $d \times d$ complex matrices. To construct MUBs, we first partition the set $\mathcal{S} \setminus \{\mathbb{I}\}$ into classes of commuting operators, with each class containing at most $(d-1)$ mutually orthogonal commuting unitary matrices.

Definition 1 (**Maximal Commuting Operator Classes**). *A set of subsets $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L | \mathcal{C}_j \subset \mathcal{S} \setminus \{\mathbb{I}\}\}$ of size $|\mathcal{C}_j| = d-1$ constitutes a partitioning of $\mathcal{S} \setminus \{\mathbb{I}\}$ into mutually disjoint maximal commuting classes if the subsets $\mathcal{C}_j$ are such that (a) the elements of $\mathcal{C}_j$ commute for all $1 \leq j \leq L$ and (b) $\mathcal{C}_j \cap \mathcal{C}_k = \emptyset$ for all $j \neq k$.*

In the rest of the paper, we often use the term *operator classes* to refer to such mutual disjoint maximal commuting classes. In particular, we use the term *Pauli classes* to refer to mutual disjoint maximal commuting classes formed out of the n-qubit Pauli group $\mathcal{P}_n$.

The correspondence between maximal commuting operator classes and MUBs is stated in the following Lemma, originally proved in [3].

Lemma 1. *The common eigenbases of L mutually disjoint maximal commuting operator classes form a set of L mutually unbiased bases.*

B. Unextendibility of MUBs and Operator Classes

Definition 2 (**Unextendible Sets of MUBs**). *A set of L MUBs $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_L\}$ is unextendible if there does not exist another basis that is unbiased with respect to the bases $\mathcal{B}_1, \ldots, \mathcal{B}_L$.*

For example, it is known that in dimension $d = 6$, the eigenbases of $\hat{X}, \hat{Z}$ and $\hat{X}\hat{Z}$ are an unextendible set of three MUBs [5], where $\hat{X}$ and $\hat{Z}$ are the generators of the Weyl-Hiesenberg group. This has the important consequence that starting with the Weyl-Hiesenberg generators we cannot hope to obtain a complete set of seven MUBs in $d = 6$. Similarly, it has been shown that the set of three MUBs in $d = 4$ constructed using Mutually Orthogonal Latin Squares [6] are also unextendible [14].

A stronger notion of unextendibility can be defined as follows.

Definition 3 (**Strongly Unextendible Sets**). *A set of L MUBs $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_L\}$ in $\mathbb{C}^d$ is said to be strongly unextendible if there does not exist any vector $v \in \mathbb{C}^d$ that is unbiased with respect to the bases $\mathcal{B}_1, \ldots, \mathcal{B}_L$.*

The eigenbases of $\hat{X}, \hat{Z}$ and $\hat{X}\hat{Z}$ in $d = 6$ are known to be strongly unextendible [5]. It is further conjectured that the set of three MUBs obtained as eigenbases of $\hat{X}, \hat{Z}$ and $\hat{X}\hat{Z}$ are strongly unextendible in any even dimension ($d = 2m$), a conjecture that has been verified for $d \leq 12$ [15].

The correspondence between MUBs and maximal commuting operator classes gives rise to a weaker notion of unextendibility, based on unextendible sets of such classes.

Definition 4 (**Unextendible Sets of Operator Classes**). *A set of L mutually disjoint maximal commuting classes $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L\}$ of operators drawn from a unitary basis $\mathcal{S}$ is said to be unextendible if no other maximal class can be formed out of the remaining operators in $\mathcal{S} \setminus (\{\mathbb{I}\} \cup \bigcup_{i=1}^{L} \mathcal{C}_i)$.*

The eigenbases of such an unextendible set of classes form a weakly unextendible set of MUBs, as defined below.

Definition 5 (**Weakly Unextendible Sets of MUBs**). *Given a set of L MUBs $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_L\}$ that are realized as common eigenbases of a set of L operator classes comprising operators from $\mathcal{S}$. The set $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_L\}$ is weakly unextendible if there does not*

exist another unbiased basis that can be realized as the common eigenbasis of a maximal commuting class of operators in $\mathcal{S}$.

For example, consider the following three Pauli classes in $d = 4$.

$$\begin{aligned} \mathcal{C}_1 &= \{Y \otimes Y, I \otimes Y, Y \otimes I\}, \\ \mathcal{C}_2 &= \{Y \otimes Z, Z \otimes X, X \otimes Y\}, \\ \mathcal{C}_3 &= \{X \otimes I, I \otimes Z, X \otimes Z\} \end{aligned} \tag{2}$$

Here, X, Y, Z denote the standard single-qubit Pauli operators. The partitioning above makes use of only nine of the fifteen two-qubit Pauli operators that constitute the set $\mathcal{P}_2 \setminus \{\mathbb{I}\}$ in $d = 4$. It is easy to check by hand that it is not possible to find one more set of 3 commuting operators from the remaining set

$$\{I \otimes X, X \otimes X, Y \otimes X, Z \otimes I, Z \otimes Y, Z \otimes Z\}$$

of six Pauli operators. The set of three classes in (2) is thus unextendible, and their common eigenbases are therefore a set of weakly unextendible MUBs. We note that this set of MUBs was obtained earlier [16] via a construction of smaller sets of MUBs in dimension $d = 2^n$ using the generators of the Clifford algebra. This set was observed to have interesting properties, in particular, saturating an entropic uncertainty relation (EUR) for the H_2 entropy. Here, we explicitly prove the tightness of the EUR using our construction of unextendible classes (see Section V B).

III. CONSTRUCTION OF UNEXTENDIBLE PAULI CLASSES IN $d = 4, 8$

In $d = 2^n$ dimensions, the set $\mathcal{P}_n \setminus \{\mathbb{I}\}$ of all tensor products of Paulis contains a total of $(4^n - 1)$ operators. As observed earlier, there exists a partitioning of these $(d^2 - 1)$ operators in $\mathcal{P}_n \setminus \{\mathbb{I}\}$ into a complete set of $(d + 1)$ mutually disjoint maximal commuting classes, with each class containing $(d-1)$ n-qubit Pauli operators. We begin by observing a few properties of such complete sets of Pauli classes which provide some intuition into our construction of unextendible Pauli classes.

(P1) Each operator in $\mathcal{P}_n \setminus \{\mathbb{I}\}$ commutes with $(\frac{4^n}{2} - 2)$ distinct operators, excluding itself and the identity operator.

(P2) Each maximal commuting class is in fact an Abelian group generated by a set of n commuting operators. The remaining operators are simply products of these n *generators*. For example, in $d = 4$, each maximal commuting class is generated by two commuting Paulis. The third element of the class is simply the product of the two generators. Similarly, in $d = 8$, every maximal commuting class is generated by three commuting operators, say, U_1, U_2, U_3. Then, the non-trivial elements in the class are given by:

$$\{U_1, U_2, U_3, U_1U_2, U_1U_3, U_2U_3, U_1U_2U_3\}$$

(P3) Given any two maximal commuting classes, the remaining $d-1$ maximal commuting classes that constitute a complete set can be realized as products of the operators in these two classes. That is, given the $d-1$ operators of $\mathcal{C}_i$ and the $d-1$ operators in $\mathcal{C}_j$ $(i, j \in [1, d+1])$, the remaining $d-1$ classes can be obtained as products of these $(d-1)^2$ operators. This fact follows from the following Lemma.

Lemma 2. *The n generators of any two maximal commuting classes that belong to a complete set of maximal commuting classes are independent of each other.*

Proof. Suppose that the n generators of a class $\mathcal{C}_i$ and the n generators of $\mathcal{C}_j$ $(j \neq i)$, are not independent of each other. This implies that at least one of the generators, say $\sigma_1^{(j)} \in \mathcal{C}_j$, can be expressed as a product of some generators $\sigma_\mu^{(i)} \in \mathcal{C}_i$ and some of the remaining $n-1$ generators of $\mathcal{C}_j$, that is, $\sigma_1^{(j)} = \sigma_1^{(i)} \dots \sigma_m^{(i)} \sigma_2^{(j)} \dots \sigma_\ell^{(j)}$. But this would mean that the non-trivial operator $\sigma_1^{(j)}\sigma_2^{(j)} \dots \sigma_\ell^{(j)} = \sigma_1^{(i)} \dots \sigma_m^{(i)}$ belongs to both $\mathcal{C}_i$ and $\mathcal{C}_j$, which are in fact disjoint sets. Thus the n generators of any two classes must be independent of each other. Note however, that if we include a third class $\mathcal{C}_k$, the generators of $\mathcal{C}_k$ can be obtained as products of the generators of $\mathcal{C}_i$ and $\mathcal{C}_j$. □

(P4) Every operator in a given class $\mathcal{C}_i$ commutes with exactly $n-1$ generators of any other class $\mathcal{C}_j$ $(j \neq i)$, and a total of $2^{n-1} - 1$ operators in the class $\mathcal{C}_j$. If an operator of $\mathcal{C}_i$ were to commute with all n generators of $\mathcal{C}_j$, it would give rise to a set of $n+1$ independent commuting operators, leading to a total of $2^{n+1} - 1$ commuting operators. Such a set cannot exist in $d = 2^n$ since the cardinality of a maximal commuting set is $2^n - 1$.

(P5) No two elements of $\mathcal{C}_i$ can commute with the same set of $2^{n-1} - 1$ operators in a different class $\mathcal{C}_j$ $(j \neq i)$. This is formally stated and proven in the following Lemma.

Lemma 3. *Every operator $U_i \in \mathcal{C}_i$ commutes with exactly $2^{n-1} - 1$ elements in any other class $\mathcal{C}_j$ $(j \neq i)$. This set of $2^{n-1} - 1$ operators is unique, that is, no two elements of $\mathcal{C}_i$ can commute with the same set of $2^{n-1} - 1$ operators in a different class $\mathcal{C}_j$ $(j \neq i)$.*

Proof. Suppose two operators $U_i, V_i \in \mathcal{C}_i$ commute with the same set of $2^{n-1} - 1$ operators in $\mathcal{C}_j$ $(j \neq i)$. This would imply that U_i, V_i commute with the same $n-1$ generators of $\mathcal{C}_j$, thus leading to a total of $n+1$ *independent* operators that all commute. These $n+1$ operators

will then generate a set of $2^{n+1}-1$ commuting operators, but such a set cannot exist in dimension $d=2^n$. Thus, no two operators of a class $\mathcal{C}_i$ can commute with the same set of $2^{n-1}-1$ operators in a different class $\mathcal{C}_j$ $(j \neq i)$. □

A. Weakly Unextendible Sets of Three MUBs in $d = 4$

We now state our central result on constructing weakly unextendible MUBs in $d=4$, and give the proof in Section A of the Appendix.

Theorem 4. *Given three classes $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$ that belong to a complete set of classes in $d=4$, there exists exactly one more maximal commuting class of operators $\mathcal{S}$ (distinct from $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$) that can be formed using the operators in $\mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3$.*

The class $\mathcal{S}$ along with the remaining two classes $\mathcal{S}_4$ and $\mathcal{S}_5$ (in the complete set) form an unextendible set of classes, whose common eigenbases form a weakly unextendible set of three MUBs.

For example, consider a complete partitioning of the two-qubit Paulis in $\mathcal{P}_2 \setminus \{\mathbb{I}\}$ as follows:

$$\begin{aligned}
\mathcal{S}_1 &= \{Z\otimes I, I\otimes Z, Z\otimes Z\} \\
\mathcal{S}_2 &= \{X\otimes I, I\otimes X, X\otimes X\} \\
\mathcal{S}_3 &= \{X\otimes Z, Z\otimes Y, Y\otimes X\} \\
\mathcal{S}_4 &= \{Y\otimes I, I\otimes Y, Y\otimes Y\} \\
\mathcal{S}_5 &= \{Y\otimes Z, Z\otimes X, X\otimes Y\}. \qquad (3)
\end{aligned}$$

The unextendible set in (2) is then constructed as follows: $\mathcal{C}_3$ is the unique Pauli class that can be formed using the operators in $\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$, whereas $\mathcal{C}_1$ and $\mathcal{C}_2$ are simply the remaining two classes $\mathcal{S}_4$ and $\mathcal{S}_5$.

Theorem 4 not only proves the existence of unextendible sets of Pauli classes in $d=4$, but provides a way to construct unextendible sets starting from any two maximal Pauli classes.

Corollary 5. *Given any two maximal commuting classes $\mathcal{C}_1$ and $\mathcal{C}_2$ in $d=4$, there always exists a third class $\mathcal{C}_3'$, of commuting operators such that the common eigenbases of $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3'$ constitute a weakly unextendible set of **three** MUBs in $d=4$.*

Proof. To see this, we first note that any two disjoint Pauli classes $\mathcal{C}_1$ and $\mathcal{C}_2$ in $d=4$ can be extended to a complete set of maximal commuting classes. Let,

$$\mathcal{C}_1 = \{U_1, V_1, U_1V_1\} \quad \text{and} \quad \mathcal{C}_2 = \{U_2, V_2, U_2V_2\}.$$

Each element in $\mathcal{C}_1$ commutes with exactly one element in $\mathcal{C}_2$. Assume without loss of generality that $[U_1, U_2] = [V_1, V_2] = [U_1V_1, U_2V_2] = 0$. The remaining three classes are then given by

$$\begin{aligned}
\mathcal{C}_3 &= \{U_1V_2, U_2V_1, U_1V_1U_2V_2\}, \\
\mathcal{C}_4 &= \{U_1U_2, V_1U_2V_2, U_1V_1V_2\}, \\
\mathcal{C}_5 &= \{U_1V_1U_2, U_1U_2V_2, V_1V_2\}.
\end{aligned}$$

Commutativity within each class can be shown by direct calculation.

Once we have the remaining three classes that form a complete set, Theorem 4 guarantees that we can form exactly one more maximal commuting class using the remaining three classes. Thus, if we construct $\mathcal{C}_3'$ following Theorem 4, by picking one element each from each of these classes, we end up with three classes whose common eigenbases are an unextendible set of three MUBs in $d=4$. □

Finally, we show that using the two-qubit Pauli operators, we cannot find any unextendible sets of **four** MUBs in $d=4$.

Theorem 6. *Given two classes $\mathcal{C}_1$ and $\mathcal{C}_2$ that belong to a complete set of maximal commuting classes, there do not exist two more classes $\mathcal{C}_3'$ and $\mathcal{C}_4'$ such that the common eigenbases of $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3'$, and $\mathcal{C}_4'$, constitute a weakly unextendible set of four MUBs in $d=4$.*

Proof. Let $\mathcal{C}_3$, $\mathcal{C}_4$ and $\mathcal{C}_5$ denote the remaining three classes of the complete set which are uniquely determined once $\mathcal{C}_1, \mathcal{C}_2$ are given. Suppose there exist $\mathcal{C}_3'$ and $\mathcal{C}_4'$ as described above. Then, $\mathcal{C}_3'$ has to be constructed from the elements of $\mathcal{C}_3$, $\mathcal{C}_4$ and $\mathcal{C}_5$. Theorem 4 implies that one can construct exactly one more maximal commuting class using the elements of $\mathcal{C}_3$, $\mathcal{C}_4$ and $\mathcal{C}_5$. Let us denote this class by $\mathcal{C}_{\text{unext}}$. Thus, $\mathcal{C}_3'$ is either the same as $\mathcal{C}_{\text{unext}}$, or it has to be one of $\mathcal{C}_3$, $\mathcal{C}_4$, or $\mathcal{C}_5$. In the former case, there cannot exist a $\mathcal{C}_4'$ such that its common eigenbasis is unbiased with respect to the other three. In the latter case, we simply recover a complete set of five MUBs, thus showing that we cannot obtain a weakly unextendible set of four MUBs starting from two classes. □

Note that Theorem 6 is a special case of [17], where it is shown that any set of d MUBs in dimension d can always be extended to a complete set.

B. Weakly Unextendible Sets of Five MUBs in $d = 8$

We next demonstrate a construction of weakly unextendible sets of MUBs in $d=8$. The basic construction idea is similar to that in $d=4$, but proving that such a construction always leads to an unextendible set turns out to be more complex in this case.

Theorem 7 (Five Weakly Unextendible MUBs in $d=8$). *Given five maximal commuting classes $\mathcal{C}_1, \ldots, \mathcal{C}_5$ that belong to a complete set of classes in dimension $d=8$, there exists exactly one more maximal commuting class that can be constructed using the elements of $\mathcal{C}_1 \cup \ldots \cup \mathcal{C}_5$. Denoting this new class as $\mathcal{S}$, $\{\mathcal{C}_6, \mathcal{C}_7, \mathcal{C}_8, \mathcal{C}_9, \mathcal{S}\}$ is a set of five unextendible Pauli classes, the common eigenbases of which form a set of weakly unextendible MUBs in $d=8$.*

We know from Lemma 3 that the only way to form a set $\mathcal{S}$ of seven commuting operators out of $\mathcal{C}_1 \cup \ldots \cup \mathcal{C}_5$ is to pick three elements from one class (say $\mathcal{C}_1$) and one element each from the remaining four classes. Furthermore, the three elements belonging to $\mathcal{C}_1$ must be of the form $\{U_i, U_j, U_iU_j\} \subset \mathcal{C}_1$. We refer to the Appendix (Section B) for a proof of Theorem 7.

The following theorem shows that starting with $k \neq 5$ classes out of a complete set, no other maximal commuting class can be formed using the operators in k such classes.

Theorem 8. *Given k maximal commuting classes $\mathcal{C}_1$, $\mathcal{C}_2$,..., $\mathcal{C}_k$ in dimension $d = 8$, it is not possible to construct another maximal commuting class using the elements of $\mathcal{C}_1 \cup \ldots \cup \mathcal{C}_k$ for $k \neq 5$.*

Once again we refer to Section B for the proof.

Together Theorems 7, and 8 imply that is possible to construct a set of exactly *five* weakly unextendible MUBs using tensor products of Paulis in $d = 8$; no more, no fewer.

C. Unextendible Sets in Higher Dimensions

The existence of unextendible sets of classes in $d = 4, 8$ relies entirely on properties (P1) through (P5) listed above, in particular, Lemma 3. Since these properties hold for all dimensions $d = 2^n$, our construction of unextendible sets of classes should generalize to higher dimensions $d = 2^n$ ($n \geq 3$) as well. However, we do not have a proof of such a general construction yet, so we will merely conjecture the existence of unextendible sets of $d/2 + 1$ MUBs here.

Conjecture 1 ($d/2 + 1$ **Unextendible MUBs in $d = 2^n$**). *Given $k = d/2 + 1$ maximal commuting classes $\mathcal{C}_1$, $\mathcal{C}_2$,..., $\mathcal{C}_{\frac{d}{2}+1}$ that belong to a complete set of maximal commuting classes in $d = 2^n$, there is exactly one more maximal commuting class $\mathcal{S}$ that can be formed using the operators of $\mathcal{C}_1 \cup \ldots \cup \mathcal{C}_{\frac{d}{2}+1}$. The set of classes $\{\mathcal{S}, \mathcal{C}_{\frac{d}{2}+2}, \mathcal{C}_{\frac{d}{2}+3}, \ldots, \mathcal{C}_{d+1}\}$ is an unextendible set of $d/2+1$ classes whose common eigenbases form an unextendible set of MUBs.*

IV. STRONGLY UNEXTENDIBLE SETS OF MUBS IN $d = 4, 8$

In the following we present examples of sets of three and five MUBs in $d = 4$ and $d = 8$ respectively, obtained from our construction, that are in fact strongly unextendible.

Consider the following two unextendible sets of Paulis in $d = 4$ and $d = 8$.

$$\begin{aligned} \mathcal{C}_1 &= \{Y \otimes Y, I \otimes Y, Y \otimes I\} \\ \mathcal{C}_2 &= \{Y \otimes Z, X \otimes X, Z \otimes Y\} \\ \mathcal{C}_3 &= \{Z \otimes I, I \otimes Z, Z \otimes Z\} \end{aligned} \quad (4)$$

$$\begin{aligned} \mathcal{C}_1 &= \{IIY, YYI, YYY, IYY, YII, IYI, YIY\}, \\ \mathcal{C}_2 &= \{IXI, XIX, XXX, IXX, IIX, XII, XXI\}, \\ \mathcal{C}_3 &= \{ZII, IZZ, ZZZ, IIZ, IZI, ZIZ, ZZI\}, \\ \mathcal{C}_4 &= \{IZX, YZI, YIX, ZYY, XYZ, ZXZ, XXY\}, \\ \mathcal{C}_5 &= \{XIZ, XYI, IYZ, ZXX, YZX, YXY, ZZY\} \end{aligned} \quad (5)$$

Suppose there exists a normalized vector $|\psi\rangle$ that is unbiased with respect to all joint eigenvectors of the given classes. Since one of the eigenbases in both sets is the computational basis we can assume that $|\psi\rangle$ is of the form

$$|\psi\rangle = \frac{1}{\sqrt{d}}(1, x_1, \ldots, x_{d-1})^T. \quad (6)$$

Denoting the joint eigenbasis of the class $\mathcal{C}_i$ by $\mathcal{B}_i = \{|b_i^{(\alpha)}\rangle : \alpha = 1, \ldots, d\}$, we get the following conditions on the vector $|\psi\rangle$:

$$|\langle\psi|b_i^{(\alpha)}\rangle|^2 - \frac{1}{d} = 0. \quad (7)$$

Note that (7) involves complex conjugation of the coefficients x_j of the vector $|\psi\rangle$.

Unbiasedness with respect to the computational basis implies that the coefficients x_j in (6) must have modulus one, which implies that $\overline{x}_j = 1/x_j$, where $\overline{x}_j$ denotes complex conjugation. Hence the left-hand side of (7) is a rational function in the $d - 1$ variables x_j. Equivalently, we can consider the system of polynomial equations obtained from the numerators of the left-hand side of (7), provided that the denominator does not vanish. It turns out that the denominators are just products of the variables x_j, so the additional condition requires that none of the variables x_j vanishes.

Using the computer algebra system Magma [18], we can compute a Gröbner basis for the ideal generated by the numerators of the conditions (7). From the Gröbner basis we can deduce that for both the sets in (4) ($d = 4$) and (5) ($d = 8$), at least two of the coefficients x_j must vanish, contradicting the assumption that $|x_j| = 1$. Hence, there does not exist a vector $|\psi\rangle$ that is unbiased to all bases, and therefore the sets of three and five MUBS in (4) ($d = 4$) and (5) ($d = 8$), respectively, are strongly unextendible.

V. APPLICATIONS OF UNEXTENDIBLE SETS IN $d = 4, 8$

Our construction of unextendible sets of classes in dimensions where a complete set of such classes exist, offers new insight into the structure of MUBs in these dimensions. The complete set of MUBs in dimensions $d = 2^n$ has $d + 1$ bases, which are optimal for state tomography, whereas the unextendible sets we construct contain $\frac{d}{2} + 1$ bases. We now discuss potential applications of such smaller sets of MUBs for quantum foundations and for cryptographic tasks.

A. State-independent Proofs of the Kochen-Specker Theorem

Consider the set of three MUBs in $d = 4$ in (2). There exists an alternate partitioning of the nine operators that constitute the set, leading to another set of three commuting classes, namely,

$$\begin{aligned} \mathcal{C}_1' &= \{Y \otimes Y, Z \otimes X, X \otimes Z\}, \\ \mathcal{C}_2' &= \{I \otimes Y, X \otimes Y, X \otimes I\}, \\ \mathcal{C}_3' &= \{Y \otimes I, Y \otimes Z, I \otimes Z\}. \end{aligned} \tag{8}$$

The new classes $\mathcal{C}_i'$ are formed by picking one commuting element each from each of $\mathcal{C}_1$, $\mathcal{C}_2$, and $\mathcal{C}_3$. Each of the nine Pauli operators in (2) is a part of two maximal commuting classes – $\mathcal{C}_i$ and $\mathcal{C}_j'$. The partitions in (2) and (8) provide two separate contexts for each of these 9 Pauli operators, thus leading to a state-independent proof of the Kochen-Specker (KS) Theorem [12] in $d = 4$, similar to the proof by Mermin [13]. In fact the set of nine two-qubit Paulis used in Mermin's original proof also give rise to an unextendible set of three MUBs, via a partitioning into an unextendible set of classes.

The existence of two such contexts for the same set of nine operators is a property unique to unextendible sets of classes in $d = 4$, as we will prove below. The existence of two such partitions of the same set of nine operators is not possible for an arbitrary triple of commuting classes that we may pick out of the complete set of five classes that exist in $d = 4$.

Theorem 9. *Given an unextendible set of three maximal commuting classes $\{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3\}$, the nine operators that constitute these classes can be partitioned into a different set of three maximal commuting classes $\{\mathcal{C}_1', \mathcal{C}_2', \mathcal{C}_3'\}$ such that $\mathcal{C}_i'$ has one operator each from each of $\mathcal{C}_1$, $\mathcal{C}_2$, and $\mathcal{C}_3$.*

Proof. Let us denote the unextendible set of three classes as

$$\begin{aligned} \mathcal{C}_1 &= \{U_1, V_1, U_1V_1\}, \\ \mathcal{C}_2 &= \{U_2, V_2, U_2V_2\}, \\ \mathcal{C}_3 &= \{U_3, V_3, U_3V_3\} \end{aligned} \tag{9}$$

If this set of three classes were in fact extendible, the operators in $\mathcal{C}_1$ and $\mathcal{C}_2$ must be distributed in such a way as to generate three more maximal commuting classes. But since these are unextendible classes, the products of the operators in $\mathcal{C}_1$ and $\mathcal{C}_2$ are distributed such that they form only one maximal commuting class, namely, $\mathcal{C}_3$. We have already encountered such a distribution in proving Theorem 4.

Let $[U_1, U_2] = 0 = [V_1, V_2]$, so that $[U_1V_1, U_2V_2] = 0$. Suppose we set $U_3 = U_1U_2$ and $V_3 = V_1V_2$, so that $U_3V_3 = U_1U_2V_1V_2$. Then, as proved in Theorem 4, the remaining product operators U_1V_2, U_2V_1, $U_1U_2V_2$, $U_2U_1V_1$, $V_1U_2V_2$, and $V_2U_1V_1$ cannot be used to form a maximal commuting class. Any other assignment of commuting products to U_3 and V_3 will lead to a complete set of maximal commuting classes. Thus the class $\mathcal{C}_3$ for an unextendible set is of the form

$$\mathcal{C}_3 = \{U_1U_2, V_1V_2, U_1U_2V_1V_2\}. \tag{10}$$

Therefore, there exist 3 other maximal commuting classes that can be formed using the operators in $\mathcal{C}_1$, $\mathcal{C}_2$, and $\mathcal{C}_3$:

$$\begin{aligned} \mathcal{C}_1' &= \{U_1, U_2, U_1U_2\}, \\ \mathcal{C}_2' &= \{V_1, V_2, V_1V_2\}, \\ \mathcal{C}_3' &= \{U_1V_1, U_2V_2, U_1U_2V_1V_2\}. \end{aligned} \tag{11}$$

□

Finally, we note that this property holds for the unextendible set in $d = 8$ given in (5). The operators constituting this set have the property that they can be partitioned into another set of five Pauli classes, as follows:

$$\begin{aligned} \mathcal{C}_1' &= \{\underbrace{IIY, YYI, YYY}_{\mathcal{C}_1}, XXI, ZZI, XXY, ZZY\}, \\ \mathcal{C}_2' &= \{\underbrace{IXI, XIX, XXX}_{\mathcal{C}_2}, ZIZ, ZXZ, YXY, YIY\}, \\ \mathcal{C}_3' &= \{\underbrace{ZII, IZZ, ZZZ}_{\mathcal{C}_3}, ZYY, ZXX, IYY, IXX\}, \\ \mathcal{C}_4' &= \{\underbrace{IZX, YZI, YIX}_{\mathcal{C}_4}, YZX, YII, IIX, IZI\}, \\ \mathcal{C}_5' &= \{\underbrace{XIZ, XYI, IYZ}_{\mathcal{C}_5}, IYI, XII, IIZ, XYZ\}. \end{aligned} \tag{12}$$

These new classes $\mathcal{C}_i'$ are obtained by picking three commuting operators from the corresponding class $\mathcal{C}_i$ in (5) and one operator each from the remaining four classes $\mathcal{C}_j$ ($j \neq i$). Thus, we have a set of operators in $d = 8$ such that every operator is part of two different maximal commuting classes. Whether this property holds in general for all unextendible sets in $d = 8$, and what role such sets play in proving violations of non-contextuality remains to be seen.

B. Tightness of H_2 Entropic Uncertainty Relation

MUBs correspond to measurement bases that are most "incompatible", where the degree of incompatibility is quantified by entropic uncertainty relations. An entropic uncertainty relation (EUR) for a set of L measurement bases $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_L\}$ provides a lower bound on the average entropy $H(B_j||\psi\rangle)$:

$$\frac{1}{L}\sum_{j=1}^{L} H(B_j||\psi\rangle) \geq c_L \ , \tag{13}$$

for all states $|\psi\rangle$. Here, $H(B_j||\psi\rangle)$ denotes the entropy of the distribution obtained by measuring state $|\psi\rangle \in$

$\mathcal{S}(\mathbb{C}^d)$ in the measurement basis $\mathcal{B}_i$. Here we will focus on the *collision entropy* H_2 of the distribution obtained by measuring state $|\psi\rangle$ in the measurement basis $\mathcal{B}_i = \{|b_i^{(j)}\rangle, j = 1, \ldots, d\}$, defined as,

$$H_2(\mathcal{B}_i||\psi\rangle) = -\log \sum_{j=1}^{d} (|\langle b_i^{(j)}|\psi\rangle|^2)^2. \tag{14}$$

For L MUBs in d dimensions, the collision entropy satisfies the following uncertainty relation [7]:

$$\frac{1}{L}\sum_{i=1}^{L} H_2(\mathcal{B}_i||\psi\rangle) \geq \log_2\left(\frac{L+d-1}{dL}\right). \tag{15}$$

However, it is not known if this EUR is tight in general. Here, we use the result of Theorem 4 to show that this uncertainty relation is in fact tight for any three MUBs in $d = 4$, whether they be (a) part of a complete set of MUBs, or (b) a set of weakly unextendible MUBs. We merely state the result here and refer to the Appendix (Section C) for the proof.

Theorem 10. *Given a set of three maximal commuting classes $\{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3\}$ in dimension $d = 4$ such that at least one more maximal commuting class $\mathcal{S}$ can be constructed by picking one element from each of $\mathcal{C}_1$, $\mathcal{C}_2$, and $\mathcal{C}_3$. Then, the common eigenstates of the operators in $\mathcal{S}$ saturate the following uncertainty relation:*

$$\frac{1}{3}\sum_{i=1}^{3} H_2(\mathcal{B}_i||\psi\rangle) \geq 1, \tag{16}$$

where $\mathcal{B}_i$ is the common eigenbasis of the operators in $\mathcal{C}_i$.

We note that such a property was observed earlier [16] for the unextendible set in (2). Here we generalize this and prove that this EUR is saturated by *all* sets for three MUBs in $d = 4$.

VI. CONCLUSIONS AND OPEN QUESTIONS

In this paper we have explored the question of whether there exist smaller, unextendible sets of mutually unbiased bases in dimensions $d = 2^n$. We have shown by explicit construction the existence of sets of $d/2 + 1$ MUBs in dimensions $d = 4, 8$ from Pauli classes, that are unextendible using common eigenbases of operator classes from the Pauli group. Our construction is based on grouping the n-qubit Pauli operators into unextendible sets of $d/2 + 1$ maximal commuting classes. We have shown that specific examples of such unextendible Pauli classes in fact lead to strongly unextendible MUBs.

Since our construction relies on general properties of a complete set of Pauli classes which hold for any $d = 2^n$, we are led to conjecture the existence of such unextendible classes in higher dimensions ($n > 3$) as well. Furthermore, since our construction essentially relies on partitioning a unitary operator basis into classes of commuting operators, it has the potential to be generalized to the case of prime-power dimensions.

In the case two-qubit systems we have pointed out an interesting connection between unextendible sets of Pauli classes and state-independent proofs of the Kochen-Specker Theorem. We have also shown that the tightness of the H_2 entropic uncertainty relation for any set of three MUBs in $d = 4$ follows as an important consequence of our construction.

We strongly suspect that the sets of weakly unextendible MUBs arising from our general construction in $d = 4, 8$ are in fact strongly unextendible. While we were able to prove this for specific examples presented in this paper, a general proof remains elusive. Furthermore, while we conjecture the existence of unextendible sets of MUBs in dimensions $d = 2^n$, proving this remains an open problem.

VII. ACKNOWLEDGMENTS

SB and WKW would like to thank The Institute of Mathematical Sciences (IMSc), Chennai, for supporting their visit during April 2012 when this work was initiated. SB would also like to thank IMSc for supporting subsequent visits related to this work and CQT, NUS, Singapore for supporting his visit in November 2012.

[1] I.D.Ivanovic, Journal of Physics A **14**, 3241 (1981).
[2] W. Wootters and B. Fields, Annals of Physics **191**, 363 (1989).
[3] S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).
[4] J. Lawrence, C. Brukner, and A. Zeilinger, Physical Review A **65**, 032320 (2002).
[5] M.Grassl, quant-ph/0406175v2 (2004).
[6] P. Wocjan and T. Beth, Quantum Information and Computation **5**, 93 (2005).
[7] S. Wehner and A. Winter, New Journal of Physics **12**, 025009 (2010).
[8] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (1984), pp. 175–179.
[9] R. Konig, S. Wehner, and J. Wullschleger, IEEE Transactions on Information Theory **58**, 1962 (2012).
[10] N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Physical Review Letters **88**, 127902 (2002).
[11] P. Mandayam and S. Wehner, Physical Review A **83**,

022329 (2011).
[12] S. Kochen and E. P. Specker, Journal of Mathematics and Mechanics **17**, 59 (1967).
[13] N. Mermin, Physical Review Letters **65**, 3373 (1990).
[14] P. Boykin, M. Sitharam, M. Tarifi, and P. Wocjan, Arxiv preprint quant-ph/0502024 (2005).
[15] M. Grassl (2009), talk at the International Conference on Quantum Foundations and Technology: Frontier and Future Shanghai, July 17-22.
[16] P. Mandayam, S. Wehner, and N. Balachandran, Journal of Mathematical Physics **51**, 082201 (2010).
[17] M. Weiner (2009), preprint arXiv:0902.0635 [math-ph].
[18] W. Bosma, J. J. Cannon, and C. Playoust, Journal of Symbolic Computation **24**, 235 (1997).
[19] Orthogonality is defined with respect to the Hilbert-Schmidt norm. Unitary operators U_i and U_j are said to be orthogonal if $\mathrm{Tr}[U_i^\dagger U_j] = 0$.

Appendix A: Proof of Theorem4

Proof. Suppose the three classes are of the form

$$\begin{aligned}\mathcal{S}_1 &= \{U_1, V_1, U_1V_1\},\\ \mathcal{S}_2 &= \{U_2, V_2, U_2V_2\},\\ \mathcal{S}_3 &= \{U_3, V_3, U_3V_3\}.\end{aligned} \tag{A1}$$

Each element is $\mathcal{S}_1$ commutes with one element from each of $\mathcal{S}_2$ and $\mathcal{S}_3$. Assume without loss of generality that $[U_1, U_2] = 0 = [U_1, U_3]$ and $[V_1, V_2] = 0 = [V_1, V_3]$. Note that V_1 and U_1 cannot both commute with the same element in $\mathcal{S}_2$ (or $\mathcal{S}_3$), for this would give a set of four commuting operators (for, e. g., $\{U_1, V_1, U_2, U_1V_1\}$), which is not possible. This immediately implies that $[U_1V_1, U_2V_2] = 0$ and $[U_1V_1, U_3V_3] = 0$.

Uniqueness: We first show that it is not possible to construct more than one maximal commuting set from the operators in $\mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3$. Suppose $U_3 = U_1U_2$ and $V_3 = V_1V_2$, so that there exist two maximal commuting sets: $\{U_1, U_2, U_1U_2\}$ and $\{V_1, V_2, V_1V_2\}$. The class $\mathcal{S}_3$ becomes

$$\mathcal{S}_3 = \{U_1U_2, V_1V_2, U_1U_2V_1V_2\}. \tag{A2}$$

Now, since *both* $[U_2, U_3] = 0$ *and* $[V_2, V_3] = 0$, we see that U_2V_2 must commute with $U_3V_3 = U_1U_2V_1V_2$. Thus, the assumption that there exists more than one maximal commuting set implies that there exists a third maximal commuting set as well — $\{U_1V_1, U_2V_2, U_3V_3\}$. We will show that this in fact leads to a contradiction.

Similar to $\mathcal{S}_3$, we can also obtain the remaining two classes $\mathcal{S}_4$ and $\mathcal{S}_5$ as products of U_1, U_2, V_1, V_2, U_1V_1, U_2V_2. Consider U_1V_2 and U_2V_1. Note that

$$\begin{aligned}[U_1V_2, U_2V_1] &= 0,\\ \text{and} \qquad (U_1V_2)(U_2V_1) &= U_1U_2V_1V_2 = U_3V_3.\end{aligned}$$

If U_1V_2, U_2V_1 were to belong to the same class, the operator U_3V_3 would occur in two different classes. Therefore, let $U_1V_2 \in \mathcal{S}_4$ and $U_2V_1 \in \mathcal{S}_5$. Next, consider the products $U_1(U_2V_2)$ and $U_2(U_1V_1)$. Since $U_1(U_2V_2) = (U_1V_2)V_2$, and we have assumed $U_1V_2 \in \mathcal{S}_4$, this operator cannot belong to $\mathcal{S}_4$. And, since

$$\begin{aligned}(U_2V_1)(U_1U_2V_2) &= -U_1V_1V_2,\\ (U_1U_2V_2)(U_2V_1) &= U_1V_1V_2,\\ \Rightarrow [U_2V_1, U_1U_2V_2] &\neq 0,\end{aligned} \tag{A3}$$

$U_1(U_2V_2)$ cannot belong to $\mathcal{S}_5$ either. Similarly, the product $U_2(U_1V_1)$ cannot belong to $\mathcal{S}_4$ or $\mathcal{S}_5$. Thus, our assumption that there exist two maximal commuting classes in $\mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3$ leads to a situation where there are not enough commuting operators to form the remaining two classes $\mathcal{S}_4$ and $\mathcal{S}_5$.

On the other hand, suppose we had assumed $U_3 = U_1V_2$ and $V_3 = U_2V_1$, we would have exactly one maximal commuting class, namely,

$$\{U_1V_1, U_2V_2, U_3V_3 = U_1U_2V_1V_2\} \tag{A4}$$

and sufficient number of commuting operators to form the remaining two classes:

$$\begin{aligned}\mathcal{S}_4 &= \{U_1U_2, V_1U_2V_2, V_2U_1V_1\},\\ \mathcal{S}_5 &= \{V_1V_2, U_1U_2V_2, U_2U_1V_1\}.\end{aligned}$$

Existence: We next show that there has to exist at least one maximal commuting class (distinct from $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$) that can be formed using the set $\{U_i, V_i, U_iV_i\}_{i=1}^3$. Once again, let $\mathcal{S}_4$ and $\mathcal{S}_5$ denote the two remaining classes that form a complete set. Consider the elements U_1V_2 and V_1V_2. These cannot belong to either $\mathcal{S}_1$ or $\mathcal{S}_2$, by construction. Suppose, $U_1U_2, V_1V_2 \notin \mathcal{S}_3$ either. Furthermore, U_1U_2 and V_1V_2 have to each belong to a different class, say $\mathcal{S}_4$ and $\mathcal{S}_5$ respectively. For, if they belonged to the same class, say $\mathcal{S}_4$, we could form more than one maximal commuting class from the operators in $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_4$, contradicting the uniqueness result above.

Now, consider the operator $U_1V_1U_2V_2$. This also cannot belong to the classes $\mathcal{S}_1$ or $\mathcal{S}_2$, by construction. Further, note that,

$$\begin{aligned}&[(U_1V_1)(U_2V_2), U_1U_2]\\ &= (U_1U_2)(U_1V_1)(U_2V_2) - (U_1V_1)(U_2V_2)(U_1U_2)\\ &= U_2(V_1V_2)U_2 - U_1(V_1V_2)U_1\end{aligned}$$

Therefore $U_1V_1U_2V_2$ commutes with U_1U_2 iff $U_1 = U_2$. Similarly, we argue that it does not commute with V_1V_2 either, implying that it cannot belong to the remaining two classes $\mathcal{S}_4$ and $\mathcal{S}_5$. Thus, $U_1V_1U_2V_2 \in \mathcal{S}_3$, leading to the existence of at least one maximal commuting class: $\{U_1V_1, U_2V_2, U_1V_1U_2V_2\}$. □

Appendix B: Five Unextendible Classes in $d = 8$

1. Proof of Theorem 7

Theorem 11 (**Five Weakly Unextendible MUBs in $d = 8$**). *Given five maximal commuting classes $\mathcal{C}_1, \ldots,$*

$\mathcal{C}_5$ which are taken from a complete set of classes in dimension $d = 8$, there exists exactly one more maximal commuting class that can be constructed using the elements of $\mathcal{C}_1 \cup \ldots \cup \mathcal{C}_5$. Denoting this new class as $\mathcal{S}$, the set $\{\mathcal{C}_6, \mathcal{C}_7, \mathcal{C}_8, \mathcal{C}_9, \mathcal{S}\}$ is a set of 5 unextendible MUBs in $d = 8$.

Proof. We know from Lemma 3 that the only way to form a set $\mathcal{S}$ of seven commuting operators out of $\mathcal{C}_1 \cup \ldots \cup \mathcal{C}_5$ is to pick three elements from one class (say $\mathcal{C}_1$) and one element each from the remaining four classes. Furthermore, the three elements belonging to $\mathcal{C}_1$ must be of the form $\{U_i, U_j, U_iU_j\} \subset \mathcal{C}_1$.

Existence: We first show that such a maximal commuting class $\mathcal{S}$ can always be found, given any five maximal commuting classes. Note that there are 7 such distinct triples that can formed using the elements of $\mathcal{C}_1$. Once we pick three operators in $\mathcal{C}_1$, there is a unique element $V_{(ij)} \in \mathcal{C}_2$ that commutes with the first three. The remaining operators in $\mathcal{S}$ will therefore have to be $U_iV_{(ij)}$, $U_jV_{(ij)}$, and $U_iU_jV_{(ij)}$. Our task is to show that at least one of the seven triples of the form $\{U_i, U_j, U_iU_j\}$ is such that the corresponding operators $U_iV_{(ij)}$, $U_jV_{(ij)}$, and $U_iU_jV_{(ij)}$ must belong to the classes $\mathcal{C}_3$, $\mathcal{C}_4$, and $\mathcal{C}_5$ respectively. This follows once we make the following observations:

(T1) The three operators $U_iV_{(ij)}$, $U_jV_{(ij)}$, and $U_iU_jV_{(ij)}$ should each belong to different class. Clearly, all three cannot belong to the same class, for that would imply that U_iU_j occurs in two different classes. No two of them can belong to the same class either, for the third is simply a product of the other two.

(T2) Let us label the seven triples that can be formed using the elements of $\mathcal{C}_1$ as τ_1, τ_2,..., τ_7. Any two of them share exactly one common element, that is, $|\tau_i \cap \tau_j| = 1$ for $i \neq j$. Consider two such triples of the form $\tau_1 = \{U_i, U_j, U_iU_j\}$ and $\tau_2 = \{U_i, U_k, U_iU_k\}$. Say $V_{(ij)} \in \mathcal{C}_2$ is the unique operator in $\mathcal{C}_2$ that commutes with τ_1, and $V_{(ik)} \in \mathcal{C}_2$ the operator that commutes with τ_2. The triples obtained by multiplying with the corresponding commuting elements in $\mathcal{C}_2$ are distributed among the remaining classes such that the operators $U_iV_{(ij)}$ and $U_iV_{(ik)}$ belong to different classes. Thus, the elements of any two triples τ_i and τ_j cannot be distributed within three classes, but need four classes.

In order to satisfy the above constraints, the operators obtained as products of the triples τ_1, τ_2, ..., τ_7 with the corresponding commuting operators in $\mathcal{C}_2$, must be distributed as follows:

$$\begin{array}{lllllll}
\tau 1 & \rightarrow & & & \mathcal{C}_6 & \mathcal{C}_7 & \mathcal{C}_8 \\
\tau 2 & \rightarrow & & & & \mathcal{C}_7 & \mathcal{C}_8 \ \mathcal{C}_9 \\
\tau 3 & \rightarrow & \mathcal{C}_3 & & & & \mathcal{C}_8 \ \mathcal{C}_9 \\
\tau 4 & \rightarrow & \mathcal{C}_3 & \mathcal{C}_4 & \mathcal{C}_5 & & \\
\tau 5 & \rightarrow & & \mathcal{C}_4 & \mathcal{C}_5 & \mathcal{C}_6 & \\
\tau 6 & \rightarrow & & & \mathcal{C}_5 & \mathcal{C}_6 & \mathcal{C}_7 \\
\tau 7 & \rightarrow & & & \mathcal{C}_6 & \mathcal{C}_7 & \mathcal{C}_8
\end{array} \tag{B1}$$

This completes our proof of the existence of at least one triple of operators $\{U_i, U_j, U_iU_j\} \in \mathcal{C}_1$ and the corresponding commuting operator $V_{(ij)} \in \mathcal{C}_2$, such that $UiV_{(ij)} \in \mathcal{C}_3$, $U_jV_{(ij)} \in \mathcal{C}_4$, $U_iU_jV_{(ij)} \in \mathcal{C}_5$. Thus, we at least one maximal commuting class $\mathcal{S}$ as desired.

Uniqueness: The distribution of triples in (B1) shows that there exists exactly one triple of the $\{U_i, U_j, U_iU_j\} \subset \mathcal{C}_1$ which can lead to a maximal commuting class $\mathcal{S}$ comprising of elements from $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \ldots \cup \mathcal{C}_5$. The question remains as to whether we can find another maximal commuting class $\mathcal{S}'$ starting with 2 generators from a class other than $\mathcal{C}_1$. We will now argue that this is impossible using the fact that $\{\mathcal{C}_1, \ldots, \mathcal{C}_5\}$ is extendible to a complete set of 9 maximal commuting classes.

We begin by noting that the complete set can be generated starting with *any* two maximal commuting classes, say $\mathcal{C}_1$ and $\mathcal{C}_2$. Let $\{A_1, A_2, A_3\}$ denote a set of generators for $\mathcal{C}_1$ and $\{B_1, B_2, B_3\}$ be a set of generators for $\mathcal{C}_2$. Each generator of $\mathcal{C}_2$ commutes with at most two generators of $\mathcal{C}_1$ and vice-versa. Without loss of generality, let us assume

$$\begin{aligned}
[A_1, B_3] &= 0 = [A_2, B_3] \\
[A_2, B_1] &= 0 = [A_3, B_1] \\
[A_3, B_2] &= 0 = [A_1, B_2]
\end{aligned}$$

Then, the generators of the remaining classes can be denoted as:

$$\begin{aligned}
\mathcal{C}_1 &\equiv \langle A_1, A_2, A_3 \rangle \\
\mathcal{C}_2 &\equiv \langle B_1, B_2, B_3 \rangle \\
\mathcal{C}_3 &\equiv \langle A_1B_1, A_2B_2, A_3B_3 \rangle \\
\mathcal{C}_4 &\equiv \langle A_1B_3, A_2(B_2B_3), A_3(B_1B_2) \rangle \\
\mathcal{C}_5 &\equiv \langle A_1B_2, A_3(B_2B_3), A_2(B_1B_2B_3) \rangle \\
\mathcal{C}_6 &\equiv \langle A_2B_1, A_1(B_2B_3), A_3(B_1B_3) \rangle \\
\mathcal{C}_7 &\equiv \langle A_2B_3, A_1(B_1B_3), A_3(B_1B_2B_3) \rangle \\
\mathcal{C}_8 &\equiv \langle A_3B_1, A_2(B_1B_2), A_1(B_1B_2B_3) \rangle \\
\mathcal{C}_9 &\equiv \langle A_3B_2, A_1(B_1B_2), A_2(B_1B_3) \rangle
\end{aligned}$$

While this construction might appear rather specific, in fact any complete set of maximal commuting classes in $d = 8$ can be realized in this fashion. In other words, given any two classes $\mathcal{C}_1$ and $\mathcal{C}_2$ in $d = 8$, we can always identify a set of generators $\{A_1, A_2, A_3\} \subset \mathcal{C}_1$ and $\{B_1, B_2, B_3\} \subset \mathcal{C}_2$ that generate the rest of the classes as described above.

Within such a realization of the complete set of maximal commuting classes, consider some set of five classes, for example, $\{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_7, \mathcal{C}_8\}$.

$$\begin{aligned}
\mathcal{C}_1 &\equiv \langle \underline{A_1}, \underline{A_2}, A_3 \rangle \\
\mathcal{C}_2 &\equiv \langle B_1, B_2, \underline{B_3} \rangle \\
\mathcal{C}_4 &\equiv \langle \underline{A_1 B_3}, A_2(B_2 B_3), A_3(B_1 B_2) \rangle \\
\mathcal{C}_7 &\equiv \langle \underline{A_2 B_3}, A_1(B_1 B_3), A_3(B_1 B_2 B_3) \rangle \qquad \text{(B2)} \\
\mathcal{C}_8 &\equiv \langle A_3 B_1, A_2(B_1 B_2), A_1(B_1 B_2 B_3) \rangle \ni \underline{(A_1 A_2) B_3}
\end{aligned}$$

As proved earlier, there exists a maximal commuting class $\mathcal{S}$ that can be formed out of the operators in these five classes. Following our construction, the class $\mathcal{S}$ is obtained by choosing the generators $A_1, A_2 \in \mathcal{C}_1$ and the commuting generator $B_3 \in \mathcal{C}_2$:

$$\mathcal{S} = \{A_1, A_2, B_3, A_1 B_3, A_2 B_3, A_1 A_2 B_3\}.$$

This explicit construction allows us to see that $\mathcal{S}$ is in fact the only maximal commuting class that can be constructed from these five classes. We have already seen that such a class cannot be formed by choosing two other generators from $\mathcal{C}_1$. Starting with two generators $B_1, B_2 \in \mathcal{C}_2$ and the commuting generator $A_3 \in \mathcal{C}_1$, the resulting class has at least one operator $A_3 B_2$ that is not contained in $\mathcal{C}_4$, $\mathcal{C}_7$ or $\mathcal{C}_8$.

Pairs of generators in the remaining classes are of three different types: (a) Suppose we choose $\{A_i(B_i B_j), A_j(B_i B_j B_k)\}$ to start with. The corresponding commuting operator in $\mathcal{C}_1$ is $A_i A_j$. Taking products, the resulting class has no operator which is only a product of the B_i's, and therefore no operator from $\mathcal{C}_2$. The resulting class therefore contains at least one operator that is outside of the given five classes. (b) Suppose we choose $\{A_i(B_i B_j), A_j(B_i B_k)\}$. The corresponding commuting operator from $\mathcal{C}_1$ is $A_i A_j A_k$, the resulting class therefore has no operator from $\mathcal{C}_2$ and cannot be formed using the operators in these five classes. (c) Choosing $\{A_i B_k, A_j(B_j B_k)\}$, the corresponding commuting generators are $A_i \in \mathcal{C}_1$ and $B_k \in \mathcal{C}_2$. But taking products, the operator $A_j B_j$ is not contained in this set of five classes. We have thus shown that it is not possible to find two generators in $\mathcal{C}_2$, $\mathcal{C}_4$, $\mathcal{C}_7$, or $\mathcal{C}_8$, such that, along with the commuting generator from $\mathcal{C}_1$, they generate a different maximal commuting class within these five classes.

Finally, we note than any set of five classes can be realized as described in Equation (B2), once the generators A_1, A_2, A_3 and B_1, B_2, B_3 are suitably identified. Our uniqueness argument is therefore completely general, and shows that there exists only one more maximal commuting class in any set of five classes in $d = 8$. □

2. Proof of Theorem 8

Theorem 12. *Given k maximal commuting classes $\mathcal{C}_1$, $\mathcal{C}_2$,..., $\mathcal{C}_k$ in dimension $d = 8$, it is not possible to construct another maximal commuting class using the elements of $\mathcal{C}_1 \cup \ldots \cup \mathcal{C}_k$ for $k \neq 5$.*

Proof. (i) $k = 3$**:** We first consider starting with $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$. Since not more than three elements in a given class can commute with a fixed element of a different class, there are only two ways to construct a maximal commuting class using the elements of $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3$:

(a) find 3 elements each from two of the classes (say $\mathcal{C}_1$ and $\mathcal{C}_2$) and one more element from $\mathcal{C}_3$ that all commute, or

(b) find 3 elements from $\mathcal{C}_1$ and 2 elements each from $\mathcal{C}_2$ and $\mathcal{C}_3$ that mutually commute.

But we know from Lemma 3 that a given set of three operators in $\mathcal{C}_1$ cannot commute with more than one element from either $\mathcal{C}_2$ or $\mathcal{C}_3$. Thus, both constructions (a) and (b) are ruled out, and hence we cannot find a fourth maximal commuting class, given three maximal commuting classes.

This preceding argument also rules out the case of $k = 2$ classes, as we cannot chose more than three elements form a given class.

(ii) $k = 4$**:** Say we start with $\mathcal{C}_1$,..., $\mathcal{C}_4$. In order to construct a maximal commuting set of 7 operators form the elements of these four classes, we will again have to find two elements in one class that commute with three elements of a different class. This is not possible, as shown in Lemma 3. Thus, given four maximal commuting classes, we cannot form a fifth class using their elements.

(iii) $k = 6$**:** Given six maximal commuting classes in $d = 8$, the only way to construct another maximal commuting class is to pick one generator each from five of the classes (say $\mathcal{C}_1$,..., $\mathcal{C}_5$), and two elements from $\mathcal{C}_6$. However, Lemma 3 implies that it is not possible to pick exactly *two* operators from a single class that commute with *one* operator in a different class, in $d = 8$. The product of the two elements from $\mathcal{C}_6$ gives a third operator in $\mathcal{C}_6$ that also commutes with the other elements, thus exceeding the limit of seven commuting Paulis.

(iv) $k = 7$: Given seven maximal commuting classes in $d = 8$, the only way to construct another maximal commuting class is to find one element in each class such that all seven of them mutually commute. Note that given seven distinct elements, at least three of them must be independent. Assume that we pick three independent elements from the first three classes, i. e., $A_1 \in \mathcal{C}_1$, $B_1 \in \mathcal{C}_2$, and $C_1 \in \mathcal{C}_3$, Then the rest of the new maximal commuting class $\mathcal{S}$ is given by the products of these three operators, that is, we have

$$\mathcal{S} = \{A_1, B_1, C_1, A_1 B_1, A_1 C_1, B_1 C_1, A_1 B_1 C_1\}.$$

Now, suppose $A_1 B_1 \in \mathcal{C}_4$. According to Lemma 3, corresponding to each element in

$\mathcal{S}$, there exist commuting triples of the form $\{A_1B_1, D_i, (A_1B_1)D_i\} \in \mathcal{C}_4$. Since $\mathcal{C}_4$ has only three independent generators — A_1B_1, D_1, and D_2 — there exist only three such triples, namely:

$$\begin{aligned}\tau_1 &= \{A_1B_1, D_1, (A_1B_1)D_1\},\\ \tau_2 &= \{A_1B_1, D_2, (A_1B_1)D_2\},\\ \tau_3 &= \{A_1B_1, D_1D_2, (A_1B_1)(D_1D_2)\}.\end{aligned}$$

Say A_1 commutes with τ_1, B_1 commutes with τ_2, and C_1 commutes with τ_3. The operator B_1C_1 has to commute with one of the triples τ_1, τ_2, or τ_3. This in turn leads to a set of four independent, commuting generators, which cannot exist in $d = 8$. For example, if B_1C_1 commutes with the operators in τ_1, D_1 commutes with A_1, A_1B_1, and B_1C_1, leading to a set of four independent operators, all of which commute.

We have therefore shown that it is not possible to construct a maximal commuting class by picking one element each from $k = 7$ such classes in $d = 8$. □

Appendix C: Tightness of H_2 Uncertainty Relation

Before we prove our result on the tightness of the entropic uncertainty relation (EUR), we introduce a parametrization of the MUB vectors obtained from commuting classes of Paulis, which will prove useful in evaluating the H_2 entropy.

1. Parameterizing MUB Vectors in Terms of Binary Strings

Given a set of maximal commuting classes of Paulis in $d = 4$, let $\sigma_i^{(j)}$ denote the jth element in the class $\mathcal{C}_i$. The vectors $\{|b_i^{(\alpha)}\rangle\}$ of the basis $\mathcal{B}_i$ corresponding to the class $\mathcal{C}_i$ can be parametrized in terms of binary strings $\vec{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$ as follows:

$$|b_i^{(\alpha)}\rangle\langle b_i^{(\alpha)}| = \frac{1}{4}\left[\mathbb{I} + \sum_{j=1}^{3}(-1)^{\alpha_j}\sigma_i^{(j)}\right], \quad \alpha_j \in \{0,1\}. \tag{C1}$$

Note that the states $|b_i^{(\alpha)}\rangle\langle b_i^{(\alpha)}|$ are guaranteed to be pure states, since they are Hermitian and for all i and α, we have

$$\mathrm{Tr}\left[|b_i^{(\alpha)}\rangle\langle b_i^{(\alpha)}|\right]^2 = \frac{4}{16}\mathrm{Tr}[\mathbb{I}] = 1 = \mathrm{Tr}\left[|b_i^{(\alpha)}\rangle\langle b_i^{(\alpha)}|\right]. \tag{C2}$$

Each basis $\mathcal{B}_i = \{|b_i^{(\alpha)}\rangle, |b_i^{(\beta)}\rangle, |b_i^{(\gamma)}\rangle, |b_i^{(\delta)}\rangle\}$ is thus parametrized by four 3-bit binary strings $\vec{\alpha}$, $\vec{\beta}$,$\vec{\gamma}$, $\vec{\delta}$ which satisfy the following property.

Lemma 13. *The binary strings $\vec{\alpha}$, $\vec{\beta}$, $\vec{\gamma}$, $\vec{\delta}$ that parametrize the vectors of a basis $\mathcal{B}_i = \{|b_i^{(\alpha)}\rangle, |b_i^{(\beta)}\rangle, |b_i^{(\gamma)}\rangle, |b_i^{(\delta)}\rangle\}$ are such that for any $j = 1, 2, 3$, the string $\alpha_j\beta_j\gamma_j\delta_j$ has Hamming weight 2.*

Proof. For any two vectors $\alpha \neq \beta$ in the basis $\mathcal{B}_i$,

$$\begin{aligned}&\langle b_i^{(\beta)}|b_i^{(\alpha)}\rangle = \delta_{\alpha\beta}\\ \Rightarrow\ &\mathrm{Tr}\left[|b_i^{(\alpha)}\rangle\langle b_i^{(\alpha)}|b_i^{(\beta)}\rangle\langle b_i^{(\beta)}|\right]\\ &\qquad = \frac{1}{16}\mathrm{Tr}\left[\mathbb{I} + \mathbb{I}\sum_{j=1}^{3}(-1)^{\alpha_j\oplus\beta_j}\right]\\ &\qquad = \frac{1}{4}\left[1 + \sum_{j=1}^{3}(-1)^{\alpha_j\oplus\beta_j}\right] = 0.\end{aligned}$$

This implies that for $\alpha \neq \beta$, the strings $\vec{\alpha}$ and $\vec{\beta}$ can coincide in only one location, i.e., there is precisely one value of i for which $\alpha_i \oplus \beta_i = 0$. A more formal statement would be that the strings $\vec{\alpha}$ and $\vec{\beta}$ have a Hamming distance of 2. The Hamming distance between two binary strings of equal length is the number of positions at which the corresponding bits are different.

Each basis $\mathcal{B}_i = \{|b_i^{(\alpha)}\rangle, |b_i^{(\beta)}\rangle, |b_i^{(\gamma)}\rangle, |b_i^{(\delta)}\rangle\}$ is thus parametrized by four 3-bit binary strings $\vec{\alpha}$, $\vec{\beta}$,$\vec{\gamma}$, $\vec{\delta}$ which are at a Hamming distance of 2 from each other. Ignoring the bit where two strings take on the same value, the remaining 2-bit strings must be at a Hamming distance of 2. Notice that for a given 2-bit string, there is a unique 2-bit string that is at Hamming distance 2 from it. Thus, if $\alpha_i \oplus \beta_i = 0$ for some $i = 1, 2, 3$, $\alpha_i \oplus \gamma_i = 0$ would imply that the remaining two bits of $\vec{\gamma}$ are the same as those of $\vec{\beta}$ making $\vec{\gamma} = \vec{\beta}$.

For a given i therefore, $\alpha_i \oplus \beta_i = 0$ would imply that $\alpha_i \oplus \gamma_i = \alpha_i \oplus \delta_i = 1$, so that the string $\alpha_i\beta_i\gamma_i\delta_i$ has exactly two 0's and two 1's. □

2. Tightness of EUR

Now we are ready to prove the tightness of the EUR for the collision entropy for sets of 3 MUBs in $d = 4$.

Theorem 14. *Assume that we are given a set of 3 maximal commuting classes $\{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3\}$ in dimension $d = 4$ such that at least one maximal commuting class $\mathcal{S}$ can be constructed by picking one element from each of $\mathcal{C}_1$, $\mathcal{C}_2$, and $\mathcal{C}_3$. Then, the common eigenstates of the operators in $\mathcal{S}$ saturate the following uncertainty relation:*

$$\frac{1}{3}\sum_{i=1}^{3} H_2(\mathcal{B}_i||\psi\rangle) \geq 1, \tag{C3}$$

where $\mathcal{B}_i$ is the common eigenbasis of the operators in $\mathcal{C}_i$.

Proof. Suppose $\{\sigma_1^{(1)}, \sigma_2^{(2)}, \sigma_3^{(3)}\}$ form a commuting set. Then, the common eigenstates of such a set can again be denoted as

$$|\psi\rangle\langle\psi| = \frac{1}{4}\left[\mathbb{I} + (-1)^{e_1}\sigma_1^{(1)} + (-1)^{e_2}\sigma_2^{(2)} + (-1)^{e_3}\sigma_3^{(3)}\right].$$

Recall that the collision entropy corresponding to measuring the state $|\psi\rangle$ in basis $\mathcal{B}_i \equiv \{|b_i^{(x)}\rangle \colon x = \alpha, \beta, \gamma, \delta\}$ is given by

$$H_2(\mathcal{B}_i||\psi\rangle) = -\log \sum_{x=\alpha,\beta,\gamma,\delta} \left(\mathrm{Tr}\left[|b_i^{(x)}\rangle\langle b_i^{(x)}|\psi\rangle\langle\psi|\right]\right)^2.$$

Expanding $|\psi\rangle$ and $\{|b_i^{(x)}\rangle\}$ in terms of the σ operators as described above, we see that for a given choice of basis i, only those coefficients in the expansion of $|\psi\rangle$ that correspond to operators in $\mathcal{C}_i$ contribute to the collision entropy. Thus, for $i = 1$,

$$\begin{aligned}
H_2(\mathcal{B}_1|\psi\rangle) &= -\log \sum_{x=\alpha,\beta,\gamma,\delta} \left(\mathrm{Tr}\left[|b_1^{(x)}\rangle\langle b_1^{(x)}|\psi\rangle\langle\psi|\right]\right)^2 \\
&= -\log \sum_{x=\alpha,\beta,\gamma,\delta} \left(\frac{1}{16}\mathrm{Tr}\left[\mathbb{I} + (-1)^{x_1\oplus e_1}\mathbb{I}\right]\right)^2 \\
&= -\log \sum_{x=\alpha,\beta,\gamma,\delta} \left(\frac{4}{16}[1 + (-1)^{x_1\oplus e_1}]\right)^2 \\
&= -\log \frac{1}{16} \sum_{x=\alpha,\beta,\gamma,\delta} \left[1 + (-1)^{x_1\oplus e_1}\right]^2.
\end{aligned}$$

Since the string $\alpha_1\beta_1\gamma_1\delta_1$ has exactly two 0's and two 1's, the expression $[1 + (-1)^{x_1\oplus e_1}]$ correspondingly takes on the values 0 and 2. Since the former property holds for any string $\alpha_i\beta_i\gamma_i\delta_i$ (for all $i \in [1, 5]$), the expression $[1 + (-1)^{x_i\oplus e_i}]$ takes on the value 0 half the time and the value 2 half the time, independent of the value of i. Therefore, for $i = 1, \ldots 5$,

$$H_2(\mathcal{B}_i||\psi\rangle) = -\log \frac{1}{16}[0 + 0 + 4 + 4] = 1.$$

□